

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

IN RE DEALER MANAGEMENT SYSTEMS)	
ANTITRUST LITIGATION, MDL 2817)	Case No. 18-cv-864
)	
_____)	Judge Robert M. Dow, Jr.
)	
This document relates to:)	
)	
<i>Authenticom, Inc. v. CDK Global, Inc., et al.,</i>)	
Case No. 18-cv-868)	
)	

MEMORANDUM OPINION AND ORDER

Before the Court are the motion to dismiss the counterclaims of Defendant/Counter-Plaintiff CDK Global, LLC [272] and the motion to dismiss the conversion counterclaim of Defendant/Counter-Plaintiff Reynolds and Reynolds Co. [277] filed by Plaintiff/Counter-Defendant Authenticom, Inc. For the reasons set forth below, the motion to dismiss the counterclaims of Defendant CDK Global, LLC [272] is granted in part and denied in part, and the motion to dismiss the conversion counterclaim of Defendant Reynolds and Reynolds Co. [277] is granted.

I. Background

A. Procedural History

Plaintiff/Counter-Defendant Authenticom, Inc. (“Authenticom”) filed this lawsuit on May 1, 2017, in the Western District of Wisconsin. At that time, Authenticom filed an emergency motion for a preliminary injunction that sought to enjoin allegedly anticompetitive practices by Defendants CDK Global, LLC (“CDK”) and Reynolds and Reynolds Co. (“Reynolds”) that Authenticom contends improperly prevented it from accessing Defendants’ respective dealer management systems (“DMS”). [*Authenticom, Inc. v. CDK Global, LLC et al.*, Case No. 18-cv-

868 (N.D. Ill.), Dkt. 5.] After extensive briefing and a two-and-a-half-day hearing, the district court granted Authenticom’s motion for a preliminary injunction and entered a preliminary injunction against each Defendant mandating that Defendants permit Authenticom to access their respective DMSs. See *Authenticom, Inc. v. CDK Glob., LLC*, 2017 WL 3017048 (W.D. Wis. July 14, 2017), vacated, 874 F.3d 1019 (7th Cir. 2017).

After Defendants appealed, the Seventh Circuit vacated the preliminary injunctions and remanded the case, finding that the district court improperly issued “preliminary injunction that [went] so far beyond a measure that [would restore] what the market would look like in the absence of the alleged violation.” *Authenticom, Inc. v. CDK Glob., LLC*, 874 F.3d 1019, 1026 (7th Cir. 2017). Specifically, the Seventh Circuit held that the preliminary injunctions improperly forced Defendants to share their respective DMSs in violation of the fundamental antitrust principle that firms generally have no duty to deal with competitors. *Id.* at 1021 (citing *Verizon Commc’ns Inc. v. Law Offices of Curtis v. Trinko*, 540 U.S. 398 (2004), *Pacific Bell Tel. Co. v. Linkline Commc’ns, Inc.*, 555 U.S. 438 (2009)). The Seventh Circuit reasoned that “[t]he proper remedy for a section 1 violation based on an agreement to restrain trade is to set the offending agreement aside,” not to impose a duty to deal. *Id.* at 1026.

After the Seventh Circuit issued its opinion, the Judicial Panel on Multidistrict Litigation (“JPML”) granted Defendants’ motion for transfer and consolidation of this case and a number of other potential tag-along lawsuits filed against Defendants. [See 1.] The JPML chose the Northern District of Illinois as the transferee court and assigned the litigation to Judge St Eve. [*Id.*] While the case was before Judge St. Eve, she issued a thorough opinion granting in part and denying in part Defendants’ Rule 12(b)(6) motions to dismiss in this case. [See *In re Dealer Mgmt. Sys.*

Antitrust Litig., 313 F. Supp. 3d 931 (N.D. Ill. 2018).] The case was reassigned to this Court on May 23, 2018. [181.]

Both CDK and Reynolds subsequently answered the complaint and filed numerous counterclaims against Authenticom. [225 (Reynolds); 229 (CDK).] Specifically, CDK and Reynolds brings counterclaims against Authenticom for damages, declaratory, injunctive, and other relief pursuant to the Computer Fraud and Abuse Act, the Digital Millennium Copyright Act, the Copyright Act, the Defend Trade Secrets Act, the Wisconsin Computer Crimes Act, the California Comprehensive Computer Data Access and Fraud Act, the Wisconsin Uniform Trade Secrets Act, and state common law, consumer protection, and related laws. Pending before the Court are Authenticom's Rule 12(b)(6) motions to dismiss [272; 277] certain of those counterclaims.

B. Factual Background¹

Given that this case already has been extensively litigated before multiple courts, the Court assumes some familiarity with the facts of this case. The Counterclaims brought by CDK and Reynolds focus on Authenticom's purported unauthorized access to their enterprise software and computing platforms for automotive dealerships and dealership groups known as Dealer Management Systems or, more commonly, DMSs. Both CDK and Reynolds allege that they have devoted substantial resources to developing, securing, and maintaining their respective DMSs. According to CDK and Reynolds, Authenticom's business model revolves around improperly gaining free access to their respective DMSs, extracting and exporting the data from those DMSs, often copying the data onto its own system, and then selling the data to third-parties (principally

¹ For purposes of the motions to dismiss, the Court accepts as true all of Counter-Plaintiffs' well-pleaded factual allegations and draws all reasonable inferences in Counter-Plaintiffs' favor. *Killingsworth v. HSBC Bank Nev., N.A.*, 507 F.3d 614, 618 (7th Cir. 2007).

vendors that provide software applications to support the dealers operations). Authenticom is able to do this by using login credentials (allegedly through unsecured means) acquired from dealers.

Authenticom does not appear to dispute that Reynolds sufficiently has alleged that Authenticom lacked authorization to access its DMS. However, a central dispute raised in Authenticom’s motion to dismiss the counterclaims of CDK is whether CDK sufficiently has alleged that Authenticom lacked authorization to access its DMS. CDK alleges that Authenticom “does not have CDK’s permission or its authorization to access or use CDK’s DMS, including on behalf of or for the purported benefit of dealers or vendors.” [229, at ¶ 35.] CDK contends that its contracts with dealers and third parties make clear that its DMS has remained the sole and exclusive property of CDK. [*Id.* at ¶ 19.] Section 6(D) of CDK’s standard DMS contract with dealers—known as the “Master Service Agreement” or “MSA”— states:

Client [*i.e.*, the dealer] shall treat as confidential and will not disclose or otherwise make available any of the CDK Products (including, without limitation, screen displays or user documentation) or any trade secrets, processes, proprietary data, information or documentation related thereto (collectively the “Confidential Information”), in any form, to any person *other than employees and agents of Client* with a need-to-know.”

[276, Ex. D (emphasis added).] The MSA also prohibits “ANY THIRD PARTY [sic] SOFTWARE TO ACCESS THE CDK DEALER MANAGEMENT SYSTEM EXCEPT AS OTHERWISE PERMITTED BY [THE] AGREEMENT.” [229, at ¶ 71.]

CDK further alleges that “Authenticom became aware that CDK objected to its unauthorized access to the CDK DMS no later than June 2015, and in all likelihood, much earlier.” [*Id.* at ¶ 82.] Supporting that assertion, CDK alleges that Authenticom has taken steps to circumvent CDK’s security measures. [See, *e.g.*, *id.* at ¶ 83.] For example, Authenticom representatives certified that they were “an authorized dealer employee” in order to access CDK’s DMS. [*Id.* at ¶¶ 84-86.] Authenticom also implemented a software tool that automatically

renewed user IDs that CDK had disabled. [*Id.* at ¶ 63.] Furthermore, Authenticom was able to modify its automated scripts to bypass a CAPTCHA (“Completely Automated Public Turing test to tell Computers and Humans Apart”) control designed by CDK to stop Authenticom’s automated access to its DMS. [*Id.* at ¶¶ 90-93.]

CDK also alleges that a CDK employee informed Authenticom’s CEO Steve Cottrell “(a) that CDK’s contracts with dealers prohibited them from providing DMS login credentials to third parties (including Authenticom) and (b) that CDK intended to prevent non-authorized access to its DMS, including Authenticom’s unlawful user ID and password access.” [*Id.* at ¶ 87.] “Mr. Cottrell responded to the effect that Authenticom refused to cease its unauthorized access or otherwise change its business practices.” [*Id.*]

Both CDK and Reynolds claim that Authenticom’s purported unauthorized access to their respective DMSs has caused them harm. CDK alleges that Authenticom misappropriated protected “CDK-created forms, accounting rules, tax tables, and proprietary tools and data compilations.” [*Id.* at ¶ 115.] The “trade secrets stored on the CDK DMS derive independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, such as other DMS providers, application providers, or third-party data extractors like Authenticom.” [*Id.* at ¶ 128.] CDK “makes efforts to maintain the secrecy of these trade secrets” and outlines such efforts in its counter-complaint. [*Id.* at ¶ 129.] Authenticom’s unauthorized access adds “to the cost of computing services that CDK must provide” to each dealer. [*Id.* at ¶ 51.] Authenticom’s data extraction methods burden “CDK’s systems with poorly constructed, inefficient and repetitive queries that extract too much data, too frequently, and during peak dealer business hours.” [*Id.* at

¶ 52.] “At times, for at least some dealers, Authenticom’s constant querying can tie up more than 50% of the DMS’s entire computing capacity.” [*Id.* at ¶ 55.]

Likewise, Reynolds alleges that “the automated scripts that Authenticom uses ‘ping’ [its] DMS with computing requests at a rate of hundreds or thousands of times per day” and are dangerous to the DMS. [226, at ¶ 99.] “That speed and volume taxes the computational and network resources of the Reynolds DMS, resulting in degradation of service for dealers and increased operational costs to Reynolds.” [*Id.*] Reynolds further alleges that “[i]t has been expensive and burdensome * * * to respond to Authenticom’s continuing technological gamesmanship and ‘Whack-A-Mole’ tactics. Reynolds has had to invest significant resources in investigating and resolving hostile integration problems caused by Authenticom—a cost that Reynolds alone has had to bear, rather than dealers, third parties, or Authenticom itself. And whenever Authenticom or another hostile integrator succeeds in circumventing all of the dedicated safeguards and resources that Reynolds has built into its system, Reynolds must devote even more resources to counteracting these breaches and attempting to prevent recurrences.” [*Id.* at ¶ 101.]

II. Legal Standard

To survive a Federal Rule of Civil Procedure (“Rule”) 12(b)(6) motion to dismiss for failure to state a claim upon which relief can be granted, the complaint first must comply with Rule 8(a) by providing “a short and plain statement of the claim showing that the pleader is entitled to relief,” Fed. R. Civ. P. 8(a)(2), such that the defendant is given “fair notice of what the * * * claim is and the grounds upon which it rests.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)) (alteration in original). Second, the factual allegations in the complaint must be sufficient to raise the possibility of relief above the “speculative level.” *E.E.O.C. v. Concentra Health Servs., Inc.*, 496 F.3d 773, 776 (7th Cir. 2007)

(quoting *Twombly*, 550 U.S. at 555). “A pleading that offers ‘labels and conclusions’ or a ‘formulaic recitation of the elements of a cause of action will not do.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 555). Dismissal for failure to state a claim under Rule 12(b)(6) is proper “when the allegations in a complaint, however true, could not raise a claim of entitlement to relief.” *Twombly*, 550 U.S. at 558. In reviewing a motion to dismiss pursuant to Rule 12(b)(6), the Court accepts as true all of Counter-Plaintiffs’ well-pleaded factual allegations and draws all reasonable inferences in Counter-Plaintiffs’ favor. *Killingsworth v. HSBC Bank Nev., N.A.*, 507 F.3d 614, 618 (7th Cir. 2007).

III. Analysis

A. Authorization to Access DMS

Authenticom argues that CDK’s counterclaims should be dismissed because CDK fails plausibly to allege that Authenticom lacked authorization to access CDK’s DMS, which Authenticom contends is a necessary factual predicate for all of CDK’s counterclaims against Authenticom. Specifically, Authenticom argues that it had authorization to access to CDK’s DMS by way of Section 6(D) of CDK’s standard DMS contract—known as the “Master Service Agreement” or “MSA”—which states:

Client shall treat as confidential and will not disclose or otherwise make available any of the CDK Products (including, without limitation, screen displays or user documentation) or any trade secrets, processes, proprietary data, information or documentation related thereto (collectively the “Confidential Information”), in any form, to any person *other than employees and agents of Client* with a need-to-know.”

[276, Ex. D (emphasis added).] Because Authenticom contends it acts as an agent of CDK’s DMS clients (*i.e.*, dealers), Authenticom contends that this contractual language establishes that it actually had authorization to access CDK’s DMS.

However, CDK alleges that Authenticom “does not have CDK’s permission or its authorization to access or use CDK’s DMS, including on behalf of or for the purported benefit of dealers or vendors.” [229, at ¶ 35.] CDK further alleges that “Authenticom became aware that CDK objected to its unauthorized access to the CDK DMS no later than June 2015, and in all likelihood, much earlier.” [*Id.* at ¶ 82.] Supporting that assertion, CDK also alleges that Authenticom has taken steps to circumvent CDK’s security measures. [See, e.g., *id.* at ¶ 83.] For example, Authenticom representatives certified that they were “an authorized dealer employee” in order to access CDK’s DMS. [*Id.* at ¶¶ 84-86.] CDK also alleges that a CDK employee informed Authenticom’s CEO Steve Cottrell that “(a) that CDK’s contracts with dealers prohibited them from providing DMS login credentials to third parties (including Authenticom) and (b) that CDK intended to prevent non-authorized access to its DMS, including Authenticom’s unlawful user ID and password access.” [*Id.* at ¶ 87.] “Mr. Cottrell responded to the effect that Authenticom refused to cease its unauthorized access or otherwise change its business practices.” [*Id.*] These allegations are sufficient to establish a lack of authorization at the motion to dismiss stage.

Authenticom counters that “[t]o support its claim of unauthorized access in the face of the plain terms of CDK’s MSA, CDK must allege facts that plausibly show that Authenticom was not acting as the dealers’ agent when it accessed the CDK DMS.” [276, at 12.] That is incorrect. While it might be defense to CDK’s claim that CDK gave Authenticom authorization by way of its contract with dealers, CDK “need not anticipate defenses and attempt to defeat them.” *Jarmuth v. City of Chicago*, 43 F. Supp. 3d 889, 893 (N.D. Ill. 2014); see also *U.S. Gypsum Co. v. Indiana Gas Co.*, 350 F.3d 623, 626 (7th Cir. 2003) (“Complaints need not anticipate or attempt to defuse potential defenses.” (citing *Gomez v. Toledo*, 446 U.S. 635 (1980))). Although “[a] litigant may plead itself out of court by alleging (and thus admitting) the ingredients of a defense,” *U.S. Gypsum*

Co. v. Indiana Gas Co., 350 F.3d 623, 626 (7th Cir. 2003) (citation omitted), CDK has not done so here. While the MSA may unambiguously provide that the employees and agents of dealer clients have authority to access CDK's DMS,² CDK's allegations do not establish that Authenticom actually was an agent of the dealers. In fact, the facts alleged suggest that the contrary is true.

To begin, Authenticom's contract with dealers makes clear that it is not an agent of the dealers. [229, at ¶ 75.] Specifically, the contract between Authenticom and the dealers, which is governed by Wisconsin law, provides:

The Parties expressly agree that they are independent contractors and do not intend for these Terms and Conditions to be interpreted as an employment agency, joint venture, or partnership relationship.

[*Authenticom, Inc. v. CDK Global, LLC et al.*, Case No. 18-cv-868 (N.D. Ill.), Dkt. 65-3, at §10.4.]

Authenticom tries to dismiss this fact by arguing that the parties' characterization of their relationship is not relevant to whether Authenticom was acting as the dealers' agent. In support of that argument, Authenticom cites to a Seventh Circuit case that held that "[r]egardless of how the two parties chose to define their relationship for remuneration, tax, employment law, or tort liability purposes," the court independently should analyze their relationship on a motion for summary judgment on a claim under the Copyright Act. *Automation By Design, Inc. v. Raybestos Prod. Co.*, 463 F.3d 749, 757 (7th Cir. 2006). In other words, the Seventh Circuit held that two parties' characterization of their agency status is not dispositive of whether there exists an agency

² Many of the cases cited by Authenticom miss the mark. For example, Authenticom cites to cases holding that an unambiguous contract controls over contrary allegations in a pleading. See *McWane, Inc. v. Crow Chicago Indus., Inc.*, 224 F.3d 582, 584 (7th Cir. 2000) ("The unambiguous contract controls over contrary allegations in the plaintiff's complaint." (citing *Charles Hester Enter., Inc. v. Illinois Founders Ins. Co.*, 499 N.E.2d 1319, 1323 (Ill. 1986))). But CDK's allegations do not contradict the MSA. Similarly, Authenticom cites to cases holding that the phrase "agents and employees" is not ambiguous. *Hernandez ex rel. Gonzalez v. Tapia*, 2010 WL 5232942, at *7 (N.D. Ill. Dec. 15, 2010) ("The phrase 'agents and employees' is not ambiguous and therefore the court will apply the plain meaning of these terms."). While the phrase "agents and employees" is not ambiguous, there is still a question regarding whether Authenticom falls within the scope of that language.

relationship as the term is used under the Copyright Act. However, the language in *Automation* indicating that the parties may choose to define their relationship for “remuneration, tax, employment law, or tort liability purposes,” indicates that the parties’ characterization of their relationship may have some relevance in other contexts. See also *K.C. 1986 Ltd. P’ship v. Reade Mfg.*, 33 F. Supp. 2d 820, 828 (W.D. Mo. 1998) (“While [the parties’] characterization of their relationship as an employer/independent contractor is not dispositive of the issue before the Court, it is probative of the intended nature of the relationship.” (citations omitted)); *Bartolotta v. Dunkin’ Brands Grp., Inc.*, 2016 WL 7104290, at *5 (N.D. Ill. Dec. 6, 2016) (“In short, while the nature and extent of control as defined in the franchise agreement is relevant, so too is the parties’ actual conduct and practice.” (citations omitted)); *Ziehlsdorf v. Am. Family Ins. Grp.*, 1990 WL 149183, at *1 (Wis. Ct. App. 1990) (“A written agreement defining the relationship as an independent contractor is also a significant factor.”). Indeed, given that Authenticom is claiming that CDK’s dealer clients gave Authenticom authorization to accesses CDK’s DMS as an agent of the dealers, the fact that the contract between Authenticom and the dealers expressly disclaims such an agency relationship certainly would be relevant.

Authenticom also argues that CDK’s reading of its contract with dealers “is wrong as a matter of law” because (1) being an independent contractor is not mutually exclusive with being an agent, and (2) Authenticom’s contract with the dealers simply states that the dealers are not entering into an “employment agency.” With respect to the first point, Authenticom cites to a Wisconsin appellate court decision stating that an “[a]gents may be either servants or independent contractors.” [276, at 15 (citing *Romero v. West Bend Mut. Ins. Co.*, 885 N.W.2d 591, 601 (Wis. Ct. App. 2016).] However, under Wisconsin law, “[a]n independent contractor is one ‘who contracts with another to do something for him but who is not controlled by the other nor subject

to the other's right to control with respect to his physical conduct.” *Westmas v. Creekside Tree Serv., Inc.*, 907 N.W.2d 68, 76 (Wis. 2018) (citing Restatement (Second) of Agency § 2(3) (1958)). The Wisconsin Supreme Court therefore has recognized that the distinction between an employee or agent on one hand and an independent contractor on the other hand “is the degree of retention by the employer or principal of the right to control the manner in which the details of the work are to be performed.” *Jahns v. Milwaukee Mut. Ins. Co.*, 155 N.W.2d 674, 676 (Wis. 1968). Although an independent contractor may be considered an agent for certain purposes under certain circumstances, there is no indication that those circumstances exist here. Specifically, where the independent contractor does not owe the principal a fiduciary duty and does not reserve any right to control the details of its work, the independent contractor is not an agent. *Id.* Because there is no indication that Authenticom owed the dealers a fiduciary duty or that the dealers reserved the right to control the details of its work in the relevant contract, the parties’ representation that they are independent contractors is a strong indication that they intended to disclaim an agency relationship.

Authenticom also argues that its disavowal of an “employment agency” relationship does not apply here because that disclaimer means only that “Authenticom is not the dealers’ employee.” [276, at 15.] But if the parties had intended to accomplish only that result, they would have said simply “employment,” not “employment agency.” Although it is not clear to the Court what is meant by the term “employment agency,” it seems very unlikely that it simply means “employment.” “[C]ontract language should be construed to give meaning to every word.” *Md. Arms Ltd. P’ship v. Connell*, 786 N.W.2d 15, 25 (Wis. 2010). CDK hypothesizes that a comma mistakenly was omitted from the agreement and that the parties intended to disavow any employment, agency, joint venture, or partnership relationship. While that conclusion is possible,

it is by no means inevitable and thus the Court takes no position on it at this time. That issue can be fleshed out through discovery. Still, as discussed above, the parties' agreement expressly states that they are independent contractors and there is no indication that Authenticom owed the dealers a fiduciary duty or that the dealers reserved any right to control the details of the independent contractor's work.

Furthermore, Authenticom's own complaint alleges that CDK's contractual terms with dealers "prohibit dealers from granting access to their data to anyone else, including data integrators such as Authenticom." [*Authenticom, Inc. v. CDK Global, LLC et al.*, Case No. 1:18-cv-00868 (N.D. Ill.), Dkt. 1, at ¶ 150.] Authenticom's argues that its allegation that CDK engaged in exclusive dealing by requiring dealers that use the CDK DMS exclusively for data integration services is legal argument and not a proper factual pleading. [276, at 14.] However, CDK is not citing to Authenticom's characterization of CDK's actions as exclusive dealing. Rather, CDK is citing to the fact that Authenticom alleges that CDK's contracts prohibit dealers from granting Authenticom access to their data, which is a factual allegation.³ Authenticom also argues that "[t]he fact that CDK invoked its MSA when it forced its dealers to deal exclusively with CDK for integration services does not change the unambiguous contract language." [276, at 14.] But the unambiguous contract language merely provides that the dealers cannot disclose or otherwise make available any of the CDK Products or proprietary information to any person other than employees and agents. It does not establish as a matter of law or fact that Authenticom falls within the scope of the term "employees and agents."

³ To the extent that Authenticom contends that its characterization of the contract requires a legal analysis, the Court expects that Authenticom would not have alleged that CDK's contracts prohibit dealers from granting Authenticom access to their data unless it had a good faith basis for doing so, which would indicate there is at the very least some ambiguity regarding the scope of the authorization.

Thus, whether Authenticom was the dealers' agent is an issue of fact not properly resolved on Authenticom's motion to dismiss. *Restoration Specialists, LLC v. Hartford Fire Ins. Co.*, 2009 WL 3147481, at *3 (N.D. Ill. Sept. 29, 2009) (“[T]he question of agency typically presents an issue of fact that seldom can be resolved at the summary judgment stage, much less on a motion to dismiss.”); *Semitek v. Monaco Coach Corp.*, 582 F. Supp. 2d 1009, 1024 (N.D. Ill. 2008) (“[W]hether an agency relationship has been established between the parties is [an issue] of fact which is not properly resolved on a motion to dismiss.” (citation omitted)).

Finally, even if Authenticom was an agent of the dealers and thereby had authority to access CDK Products, the MSA also prohibits “ANY THIRD PARTY SOFTWARE TO ACCESS THE CDK DEALER MANAGEMENT SYSTEM EXCEPT AS OTHERWISE PERMITTED BY THIS AGREEMENT.” [229, at ¶ 71.] Authenticom argues that the same language authorizing the dealers' agents to access CDK's DMS also permits it to use its software to access the CDK DMS. But the provision allowing dealers to disclose or otherwise make available CDK's products does not specifically address third party software. It therefore is not unambiguously clear that MSA authorizes Authenticom to access CDK's DMS with its software. In connection with CDK's other allegations—such as CDK's allegations regarding Authenticom's efforts to find ways of circumventing security measures CDK took to prevent Authenticom's automated access to the CDK DMS—CDK's allegations are sufficient to establish that Authenticom accessed CDK's DMS without authorization at the motion to dismiss stage.⁴

⁴ The Court notes that the parties do not sufficiently address what law applies to the agency analysis. Authenticom cites to agency law from different sources. CDK seems to assume that Wisconsin law applies because Wisconsin law applies to Authenticom's DealerVault contracts. [337, at 12-13.] However, the relevant issue is whether Authenticom is an agent of the dealers under the MSA, which is governed by Illinois law. [276-4 (MSA), at § 18(I).]

B. Computer Fraud Statutes (Counterclaim I, IV, and VI)⁵

Authenticom argues that CDK's claims under the Computer Fraud and Abuse Act ("CFAA"), the Wisconsin Computer Crimes Act ("WCCA"), and the California Comprehensive Computer Data Access and Fraud Act ("CCCDAF") fail because CDK has not sufficiently alleged that Authenticom's access to CDK's DMS was without authorization, which is necessary to state a claim under the CFAA and related state laws. See 18 U.S.C. § 1030(a)(2)(C) (CFAA providing criminal and civil penalties for anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains * * * information from any protected computer"); Wis. Stat. § 943.70(2) (also prohibiting unauthorized access); Cal. Penal Code § 502 (same). For the reasons discussed above, CDK sufficiently has alleged a lack of authorization to survive a motion to dismiss.

CDK also argues that even if the MSA allowed dealers to give Authenticom access to CDK's DMS, Authenticom's access to the DMS over CDK's express objection would still violate the CFAA and parallel state-law statutes. The Court agrees. "CFAA's phrase 'without authorization' confirms that computer owners have the power to revoke the authorizations they grant." *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1183 (N.D. Cal. 2013) (citing *In LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009)). Thus, "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability." *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016), cert. denied, 138 S. Ct. 313 (2017).

⁵ Because Authenticom only has moved to dismiss Reynolds's conversion counterclaim, references to numerical counterclaims are to the counterclaims filed by CDK, many of which are subject to Authenticom's 12(b)(6) motion.

Here, CDK alleges that by June 2015, it clearly had put Authenticom on notice that it did not have authorization to access CDK's DMS. Authenticom argues that "CDK could not revoke [the dealers'] authorization simply by telling Authenticom that it would prefer that access had not been granted." [363, at 14.] However, as Judge Easterbrook pointed out at the Seventh Circuit oral argument, the "authorization" required for lawful access under the CFAA must come from the owner of the computer system, not from anyone who happens to use the system. [256-7 at 51:7-11 ("[The CFAA] doesn't say permission by anyone. If I have an account with AOL, * * * to get access to AOL's system, you need AOL's permission, not my permission."); see also *Facebook, Inc.*, 844 F.3d at 1067, cert. denied, 138 S. Ct. 313 (2017) (finding unauthorized use where permission expressly was rescinded in a written cease and desist order).]⁶ Although dealers might have a breach of contract claim against CDK if CDK's denial of authority violated its contract with the dealers, that does not change the fact that CDK denied Authenticom authority. The Court therefore denies Authenticom's motion to dismiss CDK's claims under the CFAA, the WCCA, and the CCCDAF.

C. Digital Millennium Copyright Act (Counterclaim II)

CDK brings a counter-claim against Authenticom under the Digital Millennium Copyright Act ("DMCA"). The DMCA prohibits circumvention of a "technological measure" "without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). Authenticom argues that CDK's

⁶ Authenticom argues that *Facebook* is inapposite because the defendant in that case could not "reasonably * * * have thought" that Facebook users had the right to authorize its access once Facebook informed the defendant in a cease-and-desist letter that users did not have such a right under Facebook's terms and conditions. [363, at 14-15.] However, Authenticom misapprehends the holding of *Facebook*. In *Facebook*, the Ninth Circuit recognized that for the defendant to continue accessing Facebook's computers, the defendant "needed authorization both from individual Facebook users (who controlled their data and personal pages) and from Facebook (which stored this data on its physical servers). Permission from the users alone was not sufficient to constitute authorization after Facebook issued the cease and desist letter." 844 F.3d at 1068. Similarly, authorization from dealers alone is not sufficient. Although Authenticom may initially have believed that it had CDK's authority, CDK alleges that it later made clear to Authenticom that its access of CDK's DMS was not authorized.

DMCA claim fails on three grounds. First, Authenticom argues that CDK's DMCA claim fails because Authenticom was an authorized user. For the reasons discussed above, CDK sufficiently has alleged a lack of authorization to survive a motion to dismiss. Thus, Authenticom's contrary argument that it was an authorized user cannot be resolved on a motion to dismiss.

Second, Authenticom argues that CDK has not plausibly alleged that Authenticom "circumvent[ed] a technological measure" that "effectively controls access to a [copyrighted] work." [273, at 19 (citing 17 U.S.C. § 1201(a)(2), (b)(1)).] The DMCA defines "circumvent a technological measure" to mean "descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." *Id.* at § 1201(a)(3)(A). The DMCA further defines the term to "circumvent protection afforded by a technological measure" to mean "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure." *Id.* at § 1201(b)(2)(A). Authenticom argues that CDK's allegation that Authenticom obtained access to CDK's DMS by using dealer-provided login credentials does not establish circumvention under the DMCA.

If that is all that CDK alleged, the Court would agree that such an allegation would be insufficient to establish circumvention. See *Navistar, Inc. v. New Baltimore Garage, Inc.*, 2012 WL 4338816, at *5 (N.D. Ill. Sept. 20, 2012) ("[U]sing a password to access a copyrighted work, even without authorization, does not constitute 'circumvention' under the DMCA because it does not involve descrambling, decrypting, or otherwise avoiding, bypassing, removing, deactivating, or impairing a 'technological measure.'"). However, CDK also alleges that Authenticom implemented a software tool that automatically renewed user IDs that CDK had disabled. [229, at ¶ 63.] Authenticom cites to *Navistar* to argue that its software re-enabling passwords cannot meet the statutory definition of circumvention, which requires the defendant to "descramble a scrambled

work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure.” [363, at 15 (quoting 17 U.S.C. § 1201(a)(3)(A) (emphasis omitted).] Specifically, Authenticom cites to *Navistar* to argue that “using software’s built-in features as they were designed to operate ‘does not involve descrambling, decrypting, or otherwise avoiding, bypassing, removing, deactivating, or impairing a “technological measure.”’” [*Id.* at 15 (quoting *Navistar*, 2012 WL 4338816, at *5).] But CDK’s allegations indicate that its DMS was *not* designed to allow third-parties such as Authenticom to re-enable passwords that CDK intentionally disabled. This case therefore is unlike *Navistar*, in which the plaintiff alleged that the defendant accessed copyright protected material by simply by using a legitimate username/password combination. 2012 WL 4338816, at *4.

Furthermore, CDK alleges that Authenticom was able to modify its automated scripts in response to a CAPTCHA⁷ control designed by CDK to stop Authenticom’s automated access. [229, at ¶¶ 90-93.] Authenticom argues that its “responding” to the CAPTCHA does not establish circumvention under the DMCA because passing a CAPTCHA “does not involve descrambling, decrypting, or otherwise avoiding, bypassing, removing, deactivating, or impairing a ‘technological measure.’” [276, at 20 (quoting *Navistar*, 2012 WL 4338816, at *5).] But CDK alleges that a CAPTCHA is a security measure intended to prevent and discourage the use of automated programs. [337, at 18-19.] Authenticom’s use of an automated program to bypass CDK’s use of a CAPTCHA does avoid and/or bypass the technological measure taken by CDK to prevent the use of automated programs. See *Ticketmaster L.L.C. v. Prestige Entm’t, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018) (“By using bots or CAPTCHA farms, Defendants are ‘avoiding’ CAPTCHA without the authority of Ticketmaster.”); see also *Ticketmaster L.L.C. v.*

⁷ “CAPTCHA” is an acronym for “Completely Automated Public Turing Test to tell Computers and Humans Apart.” *Tel. Sci. Corp. v. Asset Recovery Sols., LLC*, 2016 WL 4179150, at *1 (N.D. Ill. Aug. 8, 2016).

Prestige Entm't W., Inc., 315 F. Supp. 3d 1147, 1167 (C.D. Cal. 2018); *Craigslist, Inc. v. Kerbel*, 2012 WL 3166798, at *9 (N.D. Cal. Aug. 2, 2012).⁸ Thus, CDK plausibly has alleged circumvention under the DMCA.⁹

Third, in its motion to dismiss, Authenticom argues that CDK has not plausibly alleged that Authenticom's conduct falls outside of the reverse engineering provision of 17 U.S.C. § 1201(f)(2), which precludes liability under the DMCA for those who "develop and employ technological means to circumvent a technological measure * * * for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title." 17 U.S.C. § 1201(f)(2).

CDK responds that Section 1201(f)(2) is an affirmative defense and CDK has not pled itself out of court by alleging facts establishing the elements of the affirmative defense. CDK also argues that the exception created by § 1201(f)(2) is only a defense to Section 1201(a)(2) and 1201(b)'s anti-trafficking provisions, not to Section 1201(a)(1)'s prohibition on unauthorized circumvention of technological measures. See 17 U.S.C. § 1201(f)(2) ("Notwithstanding the provisions of subsections (a)(2) and (b) * * *."). Authenticom fails to respond to these arguments

⁸ Authenticom attempts to argue that these out of circuit authorities were incorrectly decided because they focus on the intent of the technological measures taken, but the statute does not reference intent. [363, at 15.] Although CDK references intent when characterizing the CAPTCHA as a "security measure" [337, at 19-20], none of the cases relied upon by the Court discussed intent in the portions of the opinions addressing the DMCA. Still, as Authenticom recognizes, the relevant standard is whether a technological measure that effectively controls access was circumvented. [363, at 15.] Thus, to the extent that a measure is designed to control access and does so effectively, intent may be relevant.

⁹ Authenticom also argues in a footnote that CDK cannot maintain its DMCA claim based on the alleged circumvention of a CAPTCHA because "nothing in its MSA * * * would restrict a dealer's ability either to employ automated access methods itself or to authorize agents to do so on its behalf." [276, at 12 n.7.] However, nothing in the MSA specifically allows dealers to use the kind of automated access challenged by CDK and there is no indication that any dealer itself has used such automated access. Regardless, this argument only is relevant if Authenticom had authorization to act on behalf of the dealers. As discussed above, however, CDK sufficiently has alleged a lack of authorization.

and thereby has waived any arguments in response. *Bonte v. U.S. Bank, N.A.*, 624 F.3d 461, 466 (7th Cir. 2010) (“Failure to respond to an argument * * * results in waiver.” (citations omitted)).

Regardless, CDK alleges that Authenticom has done more than simply provide for interoperability between CDK’s DMS and other software programs. Specifically, CDK alleges that Authenticom extracts data from CDK’s DMS and improperly copies the data onto its own system. [229, at ¶ 41.] CDK therefore alleges that Authenticom did more than circumventing technological measures for the purposes of achieving interoperability. *Gen. Motors L.L.C. v. Autel. US Inc.*, 2016 WL 1223357, at *8 (E.D. Mich. Mar. 29, 2016) (denying motion to dismiss pursuant to the reverse engineering provision of 17 U.S.C. § 1201(f)(2) where plaintiff alleged that defendant took and copied software). Because CDK has not pled itself out of court under the reverse engineering provision of 17 U.S.C. § 1201(f)(2), the Court denies Authenticom’s motion to dismiss CDK’s DMCA claim.

D. Trade Secrets Statutes (Counterclaim III and V)

Authenticom argues that CDK’s claims brought under the federal Defend Trade Secrets Act (“DTSA”) and the Wisconsin Uniform Trade Secrets Act (“WUTSA”) should be dismissed because CDK fails to allege (1) that Authenticom engaged in actionable misappropriation and (2) the existence of legally cognizable trade secrets. See *Bay Fasteners & Components, Inc. v. Factory Direct Logistics, LLC*, 2018 WL 1394033, at *3 n.1 (N.D. Ill. Mar. 20, 2018) (recognizing that the DTSA and WUTSA are interpreted identically); *Kuryakyn Holdings, LLC v. Ciro, LLC*, 242 F. Supp. 3d 789, 797-98 (W.D. Wis. 2017) (same). For the reasons discussed below, the Court denies Authenticom’s motion to dismiss CDK’s DTSA and WUTSA claims.

To begin, CDK plausibly has alleged actionable misappropriation. The DTSA provides that “misappropriation” means the “acquisition of a trade secret of another by a person who knows

or has reason to know that the trade secret was acquired by improper means[.]” 18 U.S.C. § 1839(5). Similarly, the WUTSA provides that it is “misappropriation” to acquire “the trade secret of another by means which the person knows or has reason to know constitute improper means.” Wis. Stat. Ann. § 134.90(2)(a). “Improper means” “does not include * * * any * * * lawful means of acquisition.” 18 U.S.C. § 1839(6); see also Wis. Stat. Ann. § 134.90(2). Thus, “misappropriation of a trade secret normally is not actionable without either a tort or a breach of contract[.]” *ConFold Pac., Inc. v. Polaris Indus., Inc.*, 433 F.3d 952, 959 (7th Cir. 2006). Authenticom argues that “[a]bsent a plausible allegation that Authenticom’s access was unauthorized, CDK cannot plausibly allege knowing misappropriation by unlawful means.” [276, at 22.] However, because CDK plausibly has alleged a lack of authorization, CDK sufficiently has alleged improper means.

CDK also has sufficiently alleged the existence of legally cognizable trade secrets. “For a DTSA claim to survive a motion to dismiss, a complaint need only identify the alleged trade secret in a general sense.” *Invado Pharm., Inc. v. Forward Sci. Distribution LLC*, 2018 WL 5013556, at *3 (N.D. Ill. Oct. 16, 2018) (citations omitted). “[T]rade secrets need not be disclosed in detail in the complaint alleging misappropriation for the simple reason that such a requirement would result in public disclosure of the purported trade secrets.” *AutoMed Techs., Inc. v. Eller*, 160 F. Supp. 2d 915, 920-21 (N.D. Ill. 2001) (quoting *Leucadia, Inc. v. Applied Extrusion Techs., Inc.*, 755 F. Supp. 635, 636 (D. Del. 1991)). “At the pleading stage, plaintiffs need only describe the information and efforts to maintain the confidentiality of the information in general terms.” *Scan Top Enter. Co., Ltd. v. Winplus N. Am., Inc.*, 2015 WL 4945240, at *3 (N.D. Ill. Aug. 19, 2015). Thus, in this context, “[c]ourts only dismiss a claim for lack of specificity on the pleadings in the

most extreme cases.” *Fire ‘Em Up, Inc. v. Technocarb Equip. Ltd.*, 799 F. Supp. 2d 846, 850 (N.D. Ill. 2011) (quoting *AutoMed Techs., Inc.*, 160 F. Supp. 2d at 921 n.3).

Here, CDK alleges that its “DMS contains numerous proprietary CDK trade secrets, including forms, accounting rules, tax tables, and proprietary tools and data compilations.” [229, at ¶ 127.] CDK also explains what materials on its DMS it does not consider to be proprietary, such as data for prices and part numbers for replacement parts that would constitute proprietary data of original equipment manufacturers or “OEMs.” [*Id.* at ¶ 23.] CDK further alleges that the “trade secrets stored on the CDK DMS derive independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, such as other DMS providers, application providers, or third-party data extractors like Authenticom.” [*Id.* at ¶ 128.] CDK also alleges that it “makes efforts to maintain the secrecy of these trade secrets” and outlines such efforts. [*Id.* at ¶ 129.] Finally, CDK alleges that Authenticom misappropriated protected “CDK-created forms, accounting rules, tax tables, and proprietary tools and data compilations.” [*Id.* at ¶ 115.] These allegations suffice at the motion to dismiss stage to establish legally cognizable trade secrets. See *AutoMed Techs., Inc. v. Eller*, 160 F. Supp. 2d 915, 920-21 (N.D. Ill. 2001) (finding allegation that “software and design plans” and “Staffing Simulation program” constitute trade secrets sufficient to survive a motion to dismiss); *Wells Lamont Indus. Grp. LLC v. Richard Mendoza & Radians, Inc.*, 2017 WL 3235682, at *3 (N.D. Ill. July 31, 2017) (allegations that defendant took “substantial amounts” of confidential information such as “customer account information, product summaries, pricing sheets, product prototypes, product designs, and detailed sales reports” sufficient to survive motion to dismiss).

In its reply brief, Authenticom argues that CDK’s trade secret claims should be dismissed because Authenticom only accesses dealer data, which Authenticom argues cannot be considered CDK’s trade secret. But CDK’s allegations make clear that it is claiming that Authenticom improperly accessed “**CDK-created** forms, accounting rules, tax tables, and proprietary tools and data compilations.” [229, at ¶ 115 (emphasis added).] Although Authenticom argues that these allegations lack sufficient particularity, CDK is not required to allege its trade secrets with particularity. *Mission Measurement Corp. v. Blackbaud, Inc.*, 216 F. Supp. 3d 915, 922 (N.D. Ill. 2016) (“Defendants’ insistence that Plaintiff allege its trade secrets with ‘particularity’ is not supported by case law or the federal pleadings standards.”).

The Court recognizes that CDK’s allegations regarding the claimed trade secrets are not robust. Still, CDK’s allegations permit Authenticom to discern what trade secrets are at issue. *Cf. Chatterplug, Inc. v. Digital Intent, LLC*, 2016 WL 6395409, at *3 (N.D. Ill. Oct. 28, 2016) (finding allegation regarding trade secrets associated with specific programs insufficient where plaintiff did not even explain what the specific programs were).¹⁰ “The question of whether certain information constitutes a trade secret ordinarily is best ‘resolved by a fact finder[.]’” *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 723 (7th Cir. 2003) (quoting *Lear Siegler, Inc. v. Ark-Ell Springs, Inc.*, 569 F.2d 286, 289 (5th Cir. 1978)). Given CDK’s specific allegations regarding the location of its purported trade secrets (*i.e.*, CDK’s DMS) and its other allegations regarding

¹⁰ The only other case cited by Authenticom in which the court granted a motion to dismiss based on insufficient allegations of a legally cognizable trade secret is *Cohabaco Cigar Co. v. U.S. Tobacco Co.*, 1998 WL 773696, at *9 (N.D. Ill. Oct. 30, 1998). In that case, the court held that “allegations of defendant misappropriation of general business information, marketing plans, strategies and other ‘confidential and proprietary information’ do not satisfy the Seventh Circuit’s requirement of pleading concrete, protectable trade secrets.” *Cohabaco Cigar Co. v. U.S. Tobacco Co.*, 1998 WL 773696, at *9 (N.D. Ill. Oct. 30, 1998) (citing *Composite Marine Propellers, Inc. v. Van Der Woude*, 962 F.2d 1263, 1266 (7th Cir. 1992)). However, the Seventh Circuit decision relied upon by that court was reviewing the sufficiency of evidence presented at trial. *Composite Marine Propellers*, 962 F.2d at 1266-68. Furthermore, as discussed herein, the Court finds that CDK sufficiently has alleged legally cognizable trade secrets.

how the DMS is used and what information on its DMS it considers to be proprietary, this is not one of the “extreme cases” that warrants dismissal for a lack of specificity.

E. Tortious Interference with the MSA (Counterclaim VIII)

Authenticom argues that CDK’s tortious interference with the MSA claim fails “because it is premised on the assertion that the MSAs prohibit Authenticom from accessing the CDK DMS without CDK’s consent.” [276, at 23.] As discussed above, CDK sufficiently has alleged a lack of authorization. The Court therefore denies Authenticom’s motion to dismiss CDK’s tortious interference claim.

F. Trespass to Chattels (Counterclaim IX)

Authenticom argues that CDK’s trespass to chattels claim fails because it “is just another variant on its claim of unauthorized access to the DMS.” Under Wisconsin law (which both parties appear to assume applies to CDK’s trespass to chattels claim), trespass to chattels occurs only when “[o]ne who without a consensual or other privilege to do so” uses or interferes with the chattel in the possession of another. *Wis. Tel. Co. v. Reynolds*, 87 N.W.2d 285, 288 (Wis. 1958) (quoting Restatement (First) of Torts, § 218). Because CDK sufficiently has alleged that CDK lacked authorization to access its DMS, Authenticom’s motion to dismiss CDK’s trespass to chattels claim is denied.

G. Conversion (Counterclaim X)

Authenticom argues that the conversion claims brought by both CDK and Reynolds fail as a matter of law, but Authenticom fails to develop its argument.¹¹ “Under Wisconsin law, the tort of conversion is often defined as the wrongful exercise of dominion or control over a chattel, and

¹¹ Authenticom also argues that the conversion claim brought by CDK fails as a matter of law because Authenticom was authorized to access CDK’s DMS. For the reasons already discussed, CDK sufficiently has alleged a lack of authorization to survive a motion to dismiss.

conversion may result from a wrongful taking or a wrongful refusal to surrender property originally lawfully obtained.”¹² *Eastman Indus. v. Norlen Inc.*, 538 F. Supp. 2d 1069, 1071 (W.D. Wis. 2008) (quotations, alterations, and citation omitted). The elements of a conversion claim under Wisconsin law “are: (1) intentional control or taking of property belonging to another, (2) without the owner’s consent, (3) resulting in serious interference with the rights of the owner to possess the property.” *Conner v. Reilly*, 2017 WL 213840, at *7 (W.D. Wis. Jan. 18, 2017) (citing *Bruner v. Heritage Cos.*, 536 N.W. 2d 814 (Wis. Ct. App. 1999)). “The general rule regarding damages for conversion is that ‘the plaintiff may recover the value of the property at the time of the conversion plus interest to the date of the trial.’” *Midwestern Helicopter, LLC v. Coolbaugh*, 839 N.W.2d 167, 170 (Wis. Ct. App. 2013) (quoting *Metropolitan Sav. & Loan Ass’n v. Zuelke’s, Inc.*, 175 N.W.2d 634, 639 (Wis. 1970)).

Authenticom argues that the conversion claims brought by both CDK and Reynolds fail as a matter of law because they have not alleged that Authenticom exercised sufficient control of their respective DMSs to support a conversion claim as a matter of law. Specifically, Authenticom argues that “[d]ominion and control requires ‘such a serious violation of the other’s right of control as to justify requiring the user to pay the full value of the chattel.’” [278, at 6 (quoting Restatement (Second) of Torts § 228 cmt. d); see also 276, at 24 (quoting Restatement (Second) of Torts § 228 cmt. d).] Although Authenticom appears to be blurring the lines between the control/taking element and the serious interference element of a conversion claim under Wisconsin law, the Court agrees that neither CDK nor Reynolds has alleged such serious interference with their right to

¹²The parties appear to agree that Wisconsin law applies to the conversion claims brought by CDK and Reynolds. Still, the parties cite to cases from other jurisdictions without explaining whether those jurisdictions use the same legal standard as Wisconsin. See, e.g., *Scs Healthcare Marketing, LLC v Allergan Usa, Inc.*, 2012 WL 6565713 (N.J. Super. Ch., Bergen County Dec. 07, 2012) (applying New Jersey law).

control their respective DMSs that Authenticom may justly be required to pay the other the full value of the DMSs.

CDK alleges that “Authenticom’s repeated access to the CDK DMS seriously interfered with CDK’s possessory rights in its server systems by reducing the efficiency and efficacy of the server systems.” [229, at ¶ 166.] CDK further alleges that Authenticom’s unauthorized access adds “to the cost of computing services that CDK must provide” to each dealer. [*Id.* at ¶ 51.] CDK also alleges that “Authenticom’s data extraction methods show that Authenticom burdens CDK’s systems with poorly constructed, inefficient and repetitive queries that extract too much data, too frequently, and during peak dealer business hours.” [*Id.* at ¶ 52.] “At times, for at least some dealers, Authenticom’s constant querying can tie up more than 50% of the DMS’s entire computing capacity.” [*Id.* at ¶ 55.]

Likewise, Reynolds alleges that “the automated scripts that Authenticom uses ‘ping’[its] DMS with computing requests at a rate of hundreds or thousands of times per day” and are dangerous to the DMS.” [226, at ¶ 99.] “That speed and volume taxes the computational and network resources of the Reynolds DMS, resulting in degradation of service for dealers and increased operational costs to Reynolds.” [*Id.*] Reynolds further alleges that “[i]t has been expensive and burdensome for Reynolds to respond to Authenticom’s continuing technological gamesmanship and ‘Whack-A-Mole’ tactics. Reynolds has had to invest significant resources in investigating and resolving hostile integration problems caused by Authenticom—a cost that Reynolds alone has had to bear, rather than dealers, third parties, or Authenticom itself. And whenever Authenticom or another hostile integrator succeeds in circumventing all of the dedicated safeguards and resources that Reynolds has built into its system, Reynolds must devote even more resources to counteracting these breaches and attempting to prevent recurrences.” [*Id.* at ¶ 101.]

Reynolds also argues that “Authenticom’s relentless onslaught of unauthorized access to the DMS system seriously interfered with Reynolds’s possessory rights in its server systems by reducing the efficiency and efficacy of the server systems, thereby crowding out legitimate transactions, and Reynolds has been directly and proximately harmed thereby.” [*Id.* at ¶ 165.]

Although these allegations are sufficient to establish damages resulting from Authenticom’s alleged unauthorized access of Counter-Plaintiffs’ DMSs, these allegations are not sufficient to establish such a serious violation of their right of control as to justify requiring the Authenticom to pay the full value of the DMSs, as required to state a claim for conversion under Wisconsin law.¹³ *Midwestern Helicopter, LLC v. Coolbaugh*, 839 N.W.2d 167, 170 (Wis. Ct. App. 2013) (“The general rule regarding damages for conversion is that ‘the plaintiff may recover the value of the property at the time of the conversion plus interest to the date of the trial.’” (quoting *Metropolitan Sav. & Loan Ass’n*, 175 N.W.2d at 639)). Indeed, given that there is no indication that either CDK or Reynolds is seeking the value of their respective DMSs, CDK and Reynolds implicitly recognize that they have not alleged the kind of serious interference with their respective DMSs necessary to establish their conversion claims. Restatement (Second) of Torts § 222A, cmt. c (1965) (“In conversion the measure of damages is the full value of the chattel, at the time

¹³ Section 222A of the Restatement (Second) of Torts provides, “[i]n determining the seriousness of the interference and the justice of requiring the actor to pay the full value, the following factors are important: (a) the extent and duration of the actor’s exercise of dominion or control; (b) the actor’s intent to assert a right in fact inconsistent with the other’s right of control; (c) the actor’s good faith; (d) the extent and duration of the resulting interference with the other’s right of control; (e) the harm done to the chattel; (f) the inconvenience and expense caused to the other.” Restatement (Second) of Torts § 222A (1965). Reynolds argues that the Court should consider these factors when determining whether Authenticom sufficiently alleged its conversion claim against Reynolds under Wisconsin law. Although Wisconsin courts have adopted and applied some of the standards set forth in the Restatement for conversion claims brought under Wisconsin law (*e.g.*, the requirement that the interference be so serious as to justify payment of the full value of the chattel), Reynolds has not cited one case applying the factors identified in Section 222A to conversion claims brought under Wisconsin law. Regardless, “[n]o one factor is always predominant in determining the seriousness of the interference, or the justice of requiring the forced purchase at full value. * * * In each case the question to be asked is whether the actor has exercised such dominion and control over the chattel, and has so seriously interfered with the other’s right to control it, that in justice he should be required to buy the chattel.” Restatement (Second) of Torts § 222A, comment d (1965). As discussed above, even considering the factors identified in the restatement, neither CDK nor Reynolds has made such allegations here.

and place of the tort. When the defendant satisfies the judgment in the action for conversion, title to the chattel passes to him, so that he is in effect required to buy it at a forced judicial sale.”). Accordingly, the Court grant’s Authenticom’s motion to dismiss the conversion claims brought by both CDK and Reynolds without prejudice.

The Court also questions whether any plaintiff could state a claim for conversion of electronic records. “Conversion in Wisconsin is limited to tangible property[.]” *Weather Shield Mfg., Inc. v. Drost*, 2018 WL 3824150, at *5 (W.D. Wis. Aug. 10, 2018) (citing *Maryland Staffing Servs., Inc. v. Manpower, Inc.*, 936 F. Supp. 1494, 1507 (E.D. Wis. 1996)). Although some courts have expanded the tort of conversion to include electronic records, see, e.g., *Thyroff v. Nationwide Mut. Ins. Co.*, 864 N.E.2d 1272, 1278 (N.Y. 2008); *Aventa Learning, Inc. v. K12 Inc.*, 830 F. Supp. 2d 1083, 1105 (W.D. Wash. 2011), no Wisconsin court has expanded its common law tort of conversion to such property. Without some argument as to why the Court should expand Wisconsin’s tort of conversion, the Court is hesitant to do so. See *Epic Sys. Corp. v. Tata Consultancy Servs. Ltd.*, 2016 WL 845341, at *27 (W.D. Wis. Mar. 2, 2016) (declining to extend Wisconsin’s common law conversion tort to electronic records stored on computers in the absence of support from Wisconsin courts for such an expansion of this state’s common law). Because neither CDK nor Reynolds alleges that Authenticom exercised sufficient control of their respective DMSs to support a conversion claim as a matter of law, the Court need not resolve that issue.

H. Unjust Enrichment (Counterclaim XI)

Authenticom moves to dismiss CDK’s unjust enrichment claim for failure to identify under which state’s law it is bringing the claim. However, in its response, CDK makes clear that it is bringing its unjust enrichment claim under Wisconsin law. Although CDK’s failure to identify the controlling law is grounds for dismissal, *In re Dairy Farmers of Am., Inc. Cheese Antitrust*

Litig., 2015 WL 3988488, at *36 (N.D. Ill. June 29, 2015), doing so would be a waste of the parties’ (and the Court’s) resources, as any dismissal would be without prejudice. *Avenarius v. Eaton Corp.*, 898 F. Supp. 2d 729, 740 (D. Del. 2012) (dismissing with leave to amend).

Given that Authenticom had the opportunity to argue for dismissal under Wisconsin law, the Court turns to the substance of CDK’s unjust enrichment claim. Authenticom argues that CDK’s unjust enrichment claim fails because CDK cannot establish unjust enrichment for a purported benefit that was contractually authorized. Specifically, Authenticom argues that dealers engaged Authenticom as their agent pursuant to the express terms of their MSAs. As already discussed, however, CDK sufficiently has alleged a lack of authorization. Authenticom also argues that CDK fails to allege that it actually conferred a benefit on Authenticom, as required to state a claim for unjust enrichment under Wisconsin law. *Puttkammer v. Minth*, 266 N.W.2d 361, 363 (Wis. 1978) (recognizing “a benefit conferred upon the defendant by the plaintiff” as an element of an unjust enrichment claim under Wisconsin law). Authenticom argues that the benefits CDK alleges Authenticom received (*i.e.*, access to CDK’s DMS and payment by vendors) were conferred by dealers and vendors and not CDK. Given that Authenticom appears to be admitting that access to CDK’s DMS is a benefit—albeit one that Authenticom contends was conferred by dealers—it is not clear based on CDK’s allegations that such a benefit was the dealers’ benefit to give. Authenticom does not explain how—under Wisconsin law—it was the dealers that actually conferred access to CDK’s DMS, especially given that CDK plausibly has alleged a lack of authorization. Although Authenticom ultimately may be able to make such a showing,¹⁴ it has not

¹⁴ Indeed, if it turns out to be the case that Authenticom was acting as the dealers’ agent and that dealers were the parties that conferred the agency status necessary for Authenticom to access CDK’s DMS, it may be that it was the dealers that conferred the benefit of accessing CDK’s DMS on Authenticom.

done so at this stage. Accordingly, the Court denies Authenticom's motion to dismiss CDK's unjust enrichment claim.

I. Fraud (Counterclaim XII)

Authenticom argues that CDK's fraud claim fails because (1) CDK fails to allege a material misstatement of fact, and (2) CDK cannot plausibly allege damages from justifiable reliance. CDK's fraud claim is based on the allegation that "Authenticom has frequently and repeatedly represented to CDK that it is a human employee of a CDK dealer customer who is authorized to access the DMS." [229, at ¶ 174.] Authenticom argues that because there is no material difference between an "employee" of the dealers and an "agent" of the dealers—which Authenticom contends would be authorized to access CDK's DMS—CDK has not sufficiently alleged a material misrepresentation. However, for the reasons discussed above, the Court is unable to determine at the motion to dismiss stage whether Authenticom actually was an agent of CDK's dealer clients. Accordingly, the Court denies Authenticom's motion to dismiss CDK's fraud claim.

J. California's Unfair Competition Law (Counterclaim VII)

Authenticom argues that CDK's counter-claim under California's Unfair Competition Law ("CUCL") fails because CDK fails to allege that Authenticom engaged in unfair or unlawful conduct. "Each prong of the UCL is a separate and distinct theory of liability" and must be analyzed separately. *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1127 (9th Cir. 2009). With respect to the CUCL's "unfair" practices prong, CDK identifies two allegedly unfair practices: (1) Authenticom's "unauthorized use of DMS login credentials," and (2) its "inducement of CDK's dealer customers to breach their contracts with CDK." [229, at ¶ 146.] Authenticom argues that neither theory is plausible because Authenticom's access to the DMS was authorized under

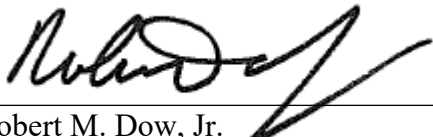
the plain terms of CDK's contract with dealers. Again, as discussed above, CDK sufficiently has alleged that Authenticom's access of CDK's DMS was not authorized.

With respect to the CUCL's "unlawful" conduct prong, Authenticom argues that CDK's CUCL claim fails because CDK has not alleged any unlawful conduct on the part of Authenticom. "The unlawful category of the UCL 'borrows violations of other laws and treats them as unlawful practices that the unfair competition law makes independently actionable.'" *Haynish v. Bank of Am., N.A.*, 284 F. Supp. 3d 1037, 1051 (N.D. Cal. 2018) (quoting *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 973 P.2d 527 (Cal. App. Ct. 1999)). "To state a claim based on an unlawful business act or practice, a plaintiff must allege facts sufficient to show a violation of some underlying law." *Johnson v. PNC Mortg.*, 2014 WL 3962662, at *11 (N.D. Cal. 2014) (citation omitted). Because CDK has alleged facts sufficient to show a violation of some underlying law (e.g., CFAA), Authenticom has alleged sufficient facts to satisfy the unlawful conduct prong of the CUCL. Accordingly, Authenticom's motion to dismiss CDK's CUCL claim is denied.

IV. Conclusion

For the reasons set forth above, the motion to dismiss counterclaims of Defendant CDK Global, LLC [272] is granted in part and denied in part, and the motion to dismiss the conversion counterclaim of Defendant Reynolds and Reynolds Co. [277] is granted.

Date: January 25, 2019



Robert M. Dow, Jr.
United States District Judge